

533 Rec'd PCT/PTO 16 AUG 2001
09/913686

Practitioner's Docket No. 13189.137

CHAPTER II

Preliminary Classification:

Proposed Class: Unknown
Subclass: Unknown

TRANSMITTAL LETTER
TO THE UNITED STATES ELECTED OFFICE (EO/US)
(ENTRY INTO U.S. NATIONAL PHASE UNDER CHAPTER II)

PCT/EP99/09981	15 December 1999 (15.12.99)	16 February 1999 (16.02.99)
International Application Number	International Filing Date	International Earliest Priority Date

TITLE OF INVENTION: METHOD AND DEVICE FOR PRODUCING AN ENCRYPTED
PAYLOAD DATA STREAM AND METHOD AND DEVICE FOR
DECRYPTING AN ENCRYPTED PAYLOAD DATA STREAM

APPLICANT(S): Rump, Niels; Koller, Juergen and Brandenburg, Karlheinz

ATTENTION: EO/US

Box PCT

Assistant Commissioner for Patents
Washington DC 20231

1. Applicant herewith submits to the United States Elected Office (EO/US) the following items under 35 U.S.C. Section 371:
 - a. This express request to immediately begin national examination procedures (35 U.S.C. Section 371(f)).
 - b. The U.S. National Fee (35 U.S.C. Section 371(c)(1)) and other fees (37 C.F.R. Section 1.492) as indicated below:

CERTIFICATION UNDER 37 C.F.R. SECTION 1.10*

(Express Mail label number is mandatory.)

(Express Mail certification is optional.)

I hereby certify that this paper, along with any document referred to, is being deposited with the United States Postal Service on this date Aug 16, 2001 in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL895408528US, addressed to ATTENTION: EO/US, Box PCT, Assistant Commissioner for Patents, Washington, DC 20231.

Cheryl Martinez

(type or print name of person mailing paper)

Cheryl Martinez
Signature of person mailing paper

WARNING: Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. Section 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

***WARNING:** Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. Section 1.10(b).
"Since the filing of correspondence under [Section] 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

Doc. 1560

09/913686

531 Rec'd PCT 16 AUG 2001

2. Fees

CLAIMS FEE*	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
BASIC FEE	TOTAL CLAIMS	31 -20 =	11	x \$18.00 =	\$198.00
	INDEPENDENT CLAIMS	4 -3 =	1	x \$80.00 =	\$80.00
	MULTIPLE DEPENDENT CLAIM(S) (if applicable) + \$270.00				\$0.00
	U.S. PTO WAS NOT INTERNATIONAL PRELIMINARY EXAMINATION AUTHORITY Where no international preliminary examination fee as set forth in Section 1.482 has been paid to the U.S. PTO, and payment of an international search fee as set forth in Section 1.445(a)(2) to the U.S. PTO: where a search report on the international application has been prepared by the European Patent Office or the Japanese Patent Office (37 C.F.R. Section 1.492(a)(5)) \$860.00				\$860.00
	Total of above Calculations				= \$1,138.00
SMALL ENTITY	Reduction by 1/2 for filing by small entity, if applicable. Affidavit must be filed. (note 37 CFR Sections 1.9, 1.27, 1.28)				- \$0.00
	Subtotal				\$1,138.00
	Total National Fee				\$1,138.00
	Fee for recording the enclosed assignment document \$40.00 (37 C.F.R. Section 1.21(h)). See attached "ASSIGNMENT COVER SHEET".				\$0.00
TOTAL	Total Fees enclosed				\$1,138.00

*See attached Preliminary Amendment Reducing the Number of Claims.

Please charge Account No. 50-1848 in the amount of \$1,138.00.

A duplicate copy of this sheet is enclosed.

3. A copy of the International Application as filed (35 U.S.C. Section 371(c)(2)) is transmitted herewith.
4. A translation of the International Application into the English language (35 U.S.C. Section 371(c)(2)) is transmitted herewith.
5. Amendments to the claims of the International application under PCT Article 19 (35 U.S.C. Section 371(c)(3)) have not been transmitted. Applicant chose not to make amendments under PCT Article 19.

Date of mailing of Search Report (from Form PCT/ISA/220): 25 July 2000.

6. A translation of the amendments to the claims under PCT Article 19 (38 U.S.C. Section 371(c)(3)) has not been transmitted for reasons indicated in section 5.

7. A copy of the International Examination Report (PCT/IPEA/416) is transmitted herewith.
8. There were no annexes to the International Preliminary Examination Report.
9. An oath or declaration of the inventor (35 U.S.C. Section 371(c)(4)) complying with 35 U.S.C. Section 115 will follow.
- II. Other document(s) or information included:
10. An International Search Report (PCT/ISA/220) or Declaration under PCT Article 17(2)(a) is transmitted herewith.
11. An Information Disclosure Statement under 37 C.F.R. Sections 1.97 and 1.98 will be transmitted within THREE MONTHS of the date of submission of requirements under 35 U.S.C. Section 371(c).
12. Additional documents:
- a. International Publication No. WO 00/49763 (Front page only)
 - b. Preliminary amendment (37 C.F.R. Section 1.121)
 - c. Final version of PCT/EP99/09981 for the prosecution at the USPTO to be filed as first preliminary amendment
 - d. Annotated copy of Final version of PCT/EP99/09981
 - e. Express Mail Certificate
 - f. Return Postcard
13. The above items are being transmitted before 30 months from any claimed priority date.

AUTHORIZATION TO CHARGE ADDITIONAL FEES

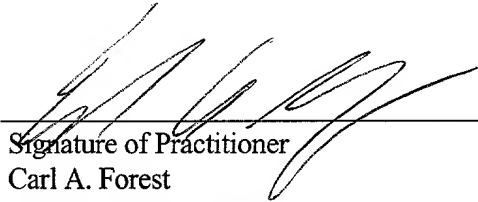
The Commissioner is hereby authorized to charge the following additional fees that may be required by this paper and during the entire pendency of this application to Account No. 50-1848:

37 C.F.R. Section 1.492(a)(1), (2), (3), and (4) (filing fees)
37 C.F.R. Section 1.492(b), (c), and (d) (presentation of extra claims)
37 C.F.R. Section 1.17 (application processing fees)
37 C.F.R. Section 1.17(a)(1)-(5) (extension fees pursuant to Section 1.136(a))
37 C.F.R. Section 1.492(e) and (f) (surcharge fees for filing the declaration and/or filing an English translation of an International Application later than 20 months after the priority date).

Date:

Aug 16, 2001

Reg. No.: 28,494
Tel. No.: 303-379-1114
Fax No.: 303-379-1155


Signature of Practitioner
Carl A. Forest
Customer No.: 24283

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
AS DESIGNATED/ELECTED OFFICE DO/EO/US

U.S. Patent Application No.: Applied For)
International Application No.: PCT/EP99/0998) Group Art Unit: Unknown
International Filing Date: 15 December 1999) Examiner: Unknown
Priority Date: 16 February 1999) Docket No: 13189.137
For: Method And Device For Producing An)
Encrypted Payload Data Stream And)
Method And Device For Decrypting An)
Encrypted Payload Data Stream)
Applicants (Inventors):)
Niels Rump, Juergen Koller and Karlhein)
Brandenburg)

ATTENTION: EO/US
BOX PCT
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, DC 20231

August 16, 2001

Dear Sir:

FIRST PRELIMINARY AMENDMENT

In the Specification:

Please substitute the attached specification entitled "Final version of PCT/EP99/09981 for the prosecution at the USPTO to be filed as first preliminary amendment" for the original PCT specification.

In the Claims:

Please substitute the enclosed claims 1 - 31, on pages 25 - 33, inclusive, attached to the substitute specification, for original claims 1 - 30.

U.S. Patent Application No.: Applied For
International Application No.: PCT/EP99/09981
First Preliminary Amendment

Page 1

Doc. 1568

In the Abstract:

Please substitute the enclosed abstract, attached to the substitute specification on page 34 for the original abstract.

REMARKS

Applicants respectfully request that the Examiner base the examination upon the attached substitute specification, claims, and abstract. An Annotated Copy Of Final Version Of PCT/EP99/09981 is enclosed showing the revisions made in the substitute specification, claims, and abstract.

The PCT specification, claims, and abstract have been revised to conform to U.S. requirements. It is believed that no new matter was introduced in revising the specification, claims, and abstract.

In view of the foregoing amendments, it is believed that the application, including claims 1 – 31 is in condition for allowance, and favorable action is respectfully requested. The Examiner is invited to contact the undersigned by collect telephone call to advance the prosecution in any respect.

No additional fee for this Preliminary Amendment is seen to be required. If any additional fee is required, please charge it to Deposit Account No. 50-1848.

Respectfully submitted,
PATTON BOGGS LLP

By: _____

Carl A. Forest, Reg. No. 28,494
Telephone: (303) 379-1114
Facsimile: (303) 379-1155
Customer No.: 24283

U.S. Patent Application No.: Applied For
International Application No.: PCT/EP99/09981
First Preliminary Amendment

Page 2

Doc. 1568

Claims

1. Method for producing a payload data stream ~~(10)~~
5 comprising a header ~~(12)~~ and a payload data block ~~(14)~~
containing encrypted payload data, comprising the
following steps:

generating ~~(102)~~ a payload data key for a payload data
10 encryption algorithm for encrypting payload data;

encrypting ~~(104)~~ payload data using said payload data
key and said payload data encryption algorithm to
obtain an encrypted section ~~(16)~~ of said payload data
15 block ~~(14)~~ of said payload data stream~~(10)~~;

processing ~~(106)~~ a part of said payload data stream
~~(10)~~ to deduce information marking said part of said
payload data stream;

20 linking ~~(108)~~ said information containing said payload
data key by means of an invertible logic linkage to
obtain a basic value;

25 encrypting ~~(110)~~ said basic value using a key of two
keys ~~(P, O)~~ being different from each other by an
asymmetrical encryption method, said two different
keys being the public ~~(O)~~ and the private ~~(P)~~ keys
respectively for said asymmetrical encryption method,
30 to obtain an output value ~~(46)~~ being an encrypted
version of said payload data key; and

entering ~~(112)~~ said output value ~~(46)~~ into said header ~~(12)~~ of said payload data stream~~(10)~~.

2. Method according to claim 1, in which said payload data encryption algorithm is a symmetrical encryption algorithm.

3. Method according to claim 1 ~~or 2~~, in which said invertible logic linkage is self-inverting and includes an XOR-linkage.

4. Method according to ~~one of the preceding claims~~ **claim 1**, in which one key of said two keys ~~(P, Q)~~ being different from each other is the private key ~~(P)~~ of a producer of said payload data stream or the public key ~~(Q)~~ of a consumer of said payload data stream.

5. Method according to ~~one of the preceding claims~~ **claim 1**, in which said part of said payload data stream being processed ~~(106)~~ to deduce said information includes at least a part of said header~~(12)~~.

6. Method according to ~~one of the preceding claims~~ **claim 1**, in which said step of processing ~~(106)~~ comprises forming a hash sum.

7. Method according to ~~one of the preceding claims~~ **claim 1**, further comprising the following step:

identifying said algorithm being used in said step of processing ~~(106)~~ by an entry ~~(68)~~ into said header.

8. Method according to ~~one of the preceding claims~~ **claim 1**, further comprising the following step:

entering license data ~~(30)~~ into said header~~(12)~~, said
5 data referring to in which way said payload data
stream ~~(10)~~ is allowed to be employed.

9. Method according to claim 8, in which said license
data ~~(30)~~ indicates how often said payload data stream
10 is allowed to be replayed ~~(58)~~ and how often it has
already been replayed~~(60)~~.

10. Method according to claim 8 ~~or 9~~, in which said
license data ~~(30)~~ indicates how often the contents of
15 said payload data stream is allowed to be copied ~~(62)~~
and how often it has already been copied~~(64)~~.

11. Method according to ~~one of claims 8 to 10~~ **claim 1**, in
which said license data ~~(30)~~ indicates from when on
20 said payload data stream is no longer allowed to be
employed~~(54)~~.

12. Method according to ~~one of claims~~ **claim 8 to 11**, in
which said license data ~~(30)~~ indicates from when on
25 said payload data stream is allowed to be
decrypted~~(56)~~.

13. Method according to ~~one of claims~~ **claim 8 to 12**, in
which said part of said payload data stream being
30 processed to deduce said information ~~(106)~~ includes
said license data~~(30)~~.

14. Method according to ~~one of the preceding claims~~ **claim 1**, in which said step of processing further comprises the following substep:

5 setting said entry ~~(46)~~ for said output value in said header ~~(12)~~ to a defined value and processing ~~(106)~~ said entire header, including said entry ~~(46)~~ set to a defined value.

10 15. Method according to ~~one of the preceding claims~~ **claim 1**, further comprising the following steps:

 identifying the supplier ~~(42)~~ of said payload data stream by a supplier entry ~~(42)~~ into said header~~(12)~~;

15 identifying the user ~~(44)~~ of said payload data stream by a user entry ~~(44)~~ into said header ~~(12)~~ of said payload data stream,

20 said supplier entry ~~(42)~~ and said user entry ~~(44)~~ belonging to said part of said payload data stream ~~(10)~~ being processed ~~(106)~~ to deduce said information.

25 16. Method according to ~~one of the preceding claims~~ **claim 1**, further comprising the following step:

 identifying said payload data encryption algorithm by an entry ~~(40)~~ into said header ~~(12)~~ of said payload data stream~~(10)~~.

30 17. Method for decrypting an encrypted payload data stream ~~(10)~~ comprising a header ~~(12)~~ and a payload data block ~~(14)~~ containing encrypted payload data, said header

(12) comprising an output value (46) having been generated by an encryption of a basic value by an asymmetrical encryption method using a key of two different keys (P, O) including a private (P) and a public (O) key, said basic value representing a linkage of a payload data key, with which said encrypted payload data is encrypted using a payload data encryption algorithm, and information deduced by a certain processing, said information marking a certain part of said payload data stream (10) unambiguously, said method comprising the following steps:

obtaining (120) said output value (46) from said header(12);

decrypting (122) said output value (46) using the other key of said asymmetrical encryption method to obtain said basic value;

processing (124) a part of said payload data stream (10) using the processing method used for encrypting to deduce information marking said part, said part corresponding to said certain part when encrypting;

linking (126) said information and said basic value using the corresponding linkage as it has been used when encrypting to obtain said payload data key; and

decrypting (128) said block (14) containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting.

18. Method according to claim 17, in which said header
(12) comprises license information (30) referring to
in what way said payload data stream (10) can be
employed.

19. Method according to claim 17 ~~or 18~~, in which said part
being processed to deduce said information is said
header(12).

20. Method according to claim 18 ~~or 19~~, further comprising
the following steps:

checking whether said license information (30) allows
a decryption; and

if a decryption is not allowed, cancelling said
decryption method.

21. Method according to ~~one of claims~~ **claim** 17 ~~to 20~~, in
which said header (12) comprises a user entry(44),
said method further comprising the following steps:

checking by means of said user entry (44) whether a
current user is authorized; and

if the user is not authorized, cancelling said
decryption method.

22. Method according to ~~one of claims~~ **claim** 17 ~~to 21~~, in
which one key having been used when encrypting is the
private key (P) of said asymmetrical encryption
method, while the other key having been used when

decrypting is the public key ~~(Q)~~ of said asymmetrical encryption method.

23. Method according to ~~one of claims claim 17 to 21~~, in
5 which one key having been used when encrypting is the public key ~~(Q)~~ of said asymmetrical encryption method, while the other key having been used when decrypting is the private key ~~(P)~~ of said asymmetrical encryption method.

24. Method according to ~~one of claims claim 17 to 23~~, in
10 which said step of processing ~~(124)~~ includes forming a hash sum.

25. Method according to ~~one of claims claim 17 to 24~~, in
15 which a part of said header ~~(12)~~ having been set to a defined value for said step of processing when encrypting is set to the same defined value for said step of processing ~~(124)~~ when decrypting.

26. Method according to claim 25, in which said part of
20 said header ~~(12)~~ being set to a defined value includes said entry for said output value ~~(46)~~ of said header~~(12)~~.

27. Method according to ~~one of claims claim 17 to 26~~, in
25 which said step of linking ~~(126)~~ comprises using an XOR-linkage.

28. Device for producing an encrypted payload data stream
30 comprising a header ~~(12)~~ and a payload data block ~~(14)~~ containing encrypted payload data, comprising:

means for generating ~~(102)~~ a payload data key for a payload data encryption algorithm for encrypting said payload data;

5 means for encrypting ~~(104)~~ payload data using said payload data key and said payload data encryption algorithm to obtain an encrypted section ~~(16)~~ of said payload data block ~~(14)~~ of said payload data stream~~(10)~~;

10 means for processing ~~(106)~~ a part of said payload data stream ~~(10)~~ to deduce information marking said part of said payload data stream;

15 means for linking ~~(108)~~ said information and said payload data key by means of an invertible logic linkage to obtain a basic value;

20 means for encrypting ~~(110)~~ said basic value using a key of two keys ~~(P, O)~~ being different from each other by an asymmetrical encryption method, said two different keys being the public ~~(O)~~ and the private ~~(P)~~ keys respectively for said asymmetrical encryption method to obtain an output value ~~(46)~~ being an
25 encrypted version of said payload data key; and

means for entering ~~(112)~~ said output value ~~(46)~~ into said header ~~(129)~~ of said payload data stream~~(10)~~.

30 ~~29~~

29. Device according to claim 28, which is implemented as a personal computer, a stereo system, a car hi-fi

instrument, a solid state player or a replay instrument containing a hard disk or a CD-ROM.

30. Device for decrypting an encrypted payload data stream
 5 ~~(10)~~ comprising a header ~~(12)~~ and a block ~~(14)~~
 containing encrypted payload data, said header ~~(12)~~
 comprising an output value ~~(46)~~ having been generated
 by an encryption of a basic value by an asymmetrical
 10 ~~(P, O)~~ including a private ~~(P)~~ and a public ~~(O)~~ key,
 said basic value representing a linkage of a payload
 data key, with which said encrypted payload data is
 encrypted using a payload data encryption algorithm,
 and information deduced by a certain processing, said
 15 information marking a certain part of said payload
 data stream ~~(10)~~ unambiguously, said device further
 comprising:

 means for obtaining ~~(120)~~ said output value ~~(46)~~ from
 20 said header~~(12)~~;

 means for decrypting ~~(122)~~ said output value ~~(46)~~
 using said other key ~~(O)~~ and said asymmetrical
 encryption method to obtain said basic value;

25 means for processing ~~(124)~~ a part of said payload data
 stream ~~(10)~~ using the processing method used when
 encrypting to deduce information marking said part,
 said part corresponding to said certain part when
 30 encrypting;

 means for linking ~~(126)~~ said information and said
 basic value using the corresponding linkage as it has

been used when encrypting to obtain said payload data key; and

means for decrypting ~~(128)~~ said block ~~(14)~~ containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting.

~~30~~

- 10 31. Device according to claim ~~28 or 29~~ 30, which is implemented as a personal computer, a stereo system, a car hi-fi instrument, a solid state player or a replay instrument containing a hard disk or a CD-ROM.

Method and device for producing an encrypted payload data
stream and method and device for decrypting an encrypted
payload data stream

5

Abstract

In a method for producing an encrypted method payload data stream comprising a header and a block containing encrypted payload data, a payload data key for a payload data encryption algorithm for encrypting payload data ~~(102)~~ is generated. The payload data is encrypted using the generated payload data key and the payload data encryption algorithm ~~(104)~~ to obtain the block containing the encrypted payload data of the payload stream. A part of the payload data stream is processed ~~(106)~~ to deduce information marking the part of the payload data stream. The information is linked ~~(108)~~ with the payload data by means of an invertible logic linkage to obtain a basic value. This basic value is finally encrypted ~~(110)~~ using a key of two keys being different from each other by an asymmetrical encryption method, the two different keys being the public and the private keys respectively for the asymmetrical encryption method to obtain an output value being an encrypted version of the payload data key. The output value is finally entered into the header to complete ~~(112)~~ the payload stream. Changes of the header and of the payload data itself, which are not authorized, lead to an automatic destruction of the payload data.

09/913686

531 Rec'd PCT/ 16 AUG 2001

National Phase of PCT/EP99/09981 in U.S.A.

Title: Method and device for producing an encrypted payload
data stream and method device for decrypting an
encrypted payload data stream

Applicants: RUMP, Niels et al.

Translation of PCT Application PCT/EP99/09981
as originally filed

00913686-0103

**Method and device for producing an encrypted payload data
stream and method device for decrypting an encrypted
payload data stream**

5

Description

10 The present invention relates to the encryption and
decryption of payload data and in particular to an
encryption concept in which the payload data is encrypted
by means of a certain key, the key being encrypted in turn
to realize a costumer-selective transmission of payload
data.

15 With the occurrence of telecommunication networks and in
particular due to the huge spreading of multimedia data-
capable personal computers and, most recently, of so-called
solid state players, a need has arisen to market digital
multimedia data, such as digital audio data and/or digital
video data, commercially. Telecommunication networks for
20 example can be analog telephone lines, digital telephone
lines, such as ISDN, or the Internet. Among the commercial
providers of multimedia products there is a need to sell or
lend multimedia data, wherein it should be possible for a
costumer to be able to select a certain product
25 individually at any time from a certain catalogue, this
product then of course being only allowed to be used by the
costumer who has paid for it.

30 Unlike well-known encrypted television programs, such as
the television channel Premiere, in which the emitted data
is encrypted in the same way for all users who have
acquired a suitable decryption device by paying a certain
charge, the present invention is to provide methods and

09/913686

devices enabling an individual, customer-selective and safe encryption and decryption of multimedia data. Unlike the television channels mentioned above which give a fixed program all of which the user has to decide for, the methods and devices of the present invention enable a maximum freedom of selection for the user, which means that the user has only to pay for those products he or she actually wants to use.

DE 196 25 635 C1 describes methods and devices for encrypting and decrypting multimedia data, the multimedia data being present in the form of an encrypted multimedia file comprising a destination data block and a payload data block. Parts of the destination data block and at least some parts of the payload data block are encrypted by means of different keys, especially symmetrical encryption methods being used.

Symmetrical encryption methods on the one hand have the advantage that they can work relatively quickly, on the other hand the user who wants to decrypt the file needs the same key as the provider, such as the German company Deutsche Telekom, who has encrypted the multimedia data to sell it to the costumer. Thus, both the provider and the user, that is the costumer, on the one hand have a table with many possible symmetrical encryption algorithms, such as DES or Blowfish, and on the other hand a table for possible keys in such a way that the provider generates an entry into the destination data block of the multimedia data, the entry being used by the user to access his key table to select the correct key for the encryption.

Due to the rapidly increasing spreading of the MP3 standard so-called solid-state-players have emerged on the market, these players being used for decrypting and replaying multimedia data. These instruments are intended to be good value and thus can only comprise a limited amount of memory space and computing power. Unlike personal computers in which the resources present exceed the resources necessary for decrypting multimedia by far, solid-state-players or stereo systems are car hi-fi instruments must be good value in order to be competitive on the hard fought for market. In addition it is necessary to relieve these instruments, concerning the computing power and memory space, as far as possible when decrypting and replaying the decrypted multimedia data. On the other hand there is still the demand that the encryption techniques used be adequately safe to be trustworthy for the customer and to prevent an abuse even of encrypted multimedia data. In addition copyright violations are to be fought effectively, especially when multimedia data is replayed without an authorization by the author or the commercialisation company respectively or when it is changed without having an authorization to do so.

It is the object of the present invention to create an efficient and safe concept for encrypting and decrypting of multimedia data respectively.

This object is achieved by a method for producing an encrypted multimedia data stream according to claim 1, a method for decrypting an encrypted multimedia data stream according to claim 17, a device for producing an encrypted multimedia data stream according to claim 26 and a device

for decrypting an encrypted multimedia data stream according to claim 28.

5 The present invention is based on the fact that a so-called hybrid encryption method has to be used in order to achieve a safe and efficient encryption, wherein the faster, for example symmetrical, encryption method or scrambling method is used for encrypting and decrypting the payload data respectively, while the slower, asymmetrical encryption concept is only used to encrypt the payload data key for the symmetrical encryption concept for example and to transmit it in this encrypted form to a user so that the user in turn can decrypt the encrypted payload data stream. Furthermore the encrypted payload data stream, which on the one hand can be a payload file or on the other hand a continuous data stream, is to be protected from illegal manipulations. In order to realize this in an efficient way and, as far as computing time is concerned, as time-saving as possible, the payload data stream itself is included in the asymmetrical encryption method for encrypting the payload data key.

It is pointed out at this stage that payload data in general includes multimedia data, that is audio data, video data or a combination of audio data and video data, but also text data for example and even binary data, such as for example executable programs. For practical reasons the subject matter of the present invention will be disclosed using multimedia data. It is however clear that all the payload data for which there is a demand for encryption can be processed by the devices and methods according to the invention.

A hash sum of a part of the multimedia data stream is preferable produced. This part could on the one hand be the header of the multimedia stream only and, on the other hand, also include parts of the encrypted and decrypted multimedia data itself.

An output value in the header which is transmitted to the customer, along with the at least partly encrypted multimedia data, in the form of multimedia data stream in a certain sense represents an encrypted version of the multimedia key, wherein to decrypt this output value again correctly to obtain the multimedia data key, apart from the key for the asymmetrical encryption method, this can be individual data created by the provider, such as license data which refers to the way how a user is allowed to use the encrypted multimedia data, as well as parts of the multimedia data itself. If a user manipulates the header by changing the expiration date of his license to use a certain piece of multimedia for example, he can on no account find out the correct key for decrypting the encrypted multimedia data since a correct decryption of the output value will no longer be possible.

It is a substantial advantage of the method that, as soon as somebody changes the header, the hash sum on the header changes, too. Thus it is no longer possible to find out the key for decrypting the multimedia data correctly. Thus any change of the header automatically leads to the destruction of the multimedia data itself.

30

This "implicit" protection of the header does not include an encryption of the header, which is why it does not have to be decrypted, a fact that in turn can be made use of for

saving resources in the replay instruments. Of course such an encryption of the header would easily be possible if there were the wish to do so.

5 In an analog way a change of the multimedia data, when encrypted or unencrypted multimedia data itself is included in the encryption of the multimedia data key, leads to an automatic destruction of all the multimedia data.

10 Preferred embodiments of the present invention are hereinafter described in detail referring to the appended drawings, in which:

15 Fig. 1 shows a multimedia data stream which can be produced according to the present invention;

Fig. 2 shows a detailed illustration of the header and the payload data block of the encrypted multimedia data stream;

20 Fig. 3 shows a selection of certain entries into the individual subblocks of the header block;

25 Fig. 4 shows a flow chart of the method for producing an encrypted multimedia data stream according to the present invention, which is preferable carried out at a distributor, that is a provider, of multimedia data; and

30 Fig. 5 shows a method for decrypting an encrypted multimedia data stream according to the present invention, which is preferable carried out at the customer or user of the multimedia data.

Fig. 1 shows an encrypted multimedia data stream 10 comprising a header 12 and a payload data block 14, that is a block containing encrypted multimedia data. The payload data block 14 includes encrypted sections 16 and unencrypted sections 18 between the encrypted sections 16. In addition a multimedia data stream which can be produced according to the present invention includes a further unencrypted section 20 following the header 12 and being arranged in front of an encrypted section 16.

Usually the multimedia data to be encrypted is encoded in any way, such as according to a MPEG standard, such as MPEG-2 AAC, MPEG-4 audio or MPEG Layer-3. It is thus sufficient to encrypt certain sections of the multimedia data to be encrypted. This leads to an essentially decreased processing expenditure both at the provider who encrypts the data and at the customer who in turn has to decrypt the data. Furthermore, the pleasure of hearing and seeing respectively of a user who only uses the unencrypted multimedia data is seriously impaired by the constantly occurring encrypted blocks, when the multimedia data is only encrypted partly.

Although Fig. 1 shows an encrypted multimedia data stream in which the header 12 is arranged at the beginning of the encrypted multimedia data stream this arrangement of the header and the payload data block is not to refer to the transmission of the encrypted multimedia data stream. The term "header" is only meant to express that a decryption device which is to decrypt the encrypted multimedia data stream at first requires at least parts of the header before the multimedia data itself can be decrypted.

Depending on the transmission medium the header may also be arranged at some place in the payload data block or be received after certain parts of the payload data block when for example a packet-oriented transmission of the multimedia data stream is thought of, in which different packets, one of which may contain the header and another one a part of the payload data block, are transmitted via different physical transmission ways in such a way that the order of receipt does not have to correspond to the order of sending. However, in this case a decryption device has to be able to save the packets received and to order them again in such a way that information is extracted from the header to begin the decryption. The encrypted multimedia data stream may further be present in the form of a file or also in the form of an actual data stream, when for example a live transmission of a multimedia event is thought of. This application will especially occur with digital user-selective broadcasting.

The length of an encrypted section 16 is represented by a value amount 22 while the spacing in the encrypted multimedia data stream from the beginning of an encrypted section 16 to the beginning of the next encrypted section 16 is referred to as step 24. The length of the further encrypted section 20 is given by a value first step 26.

These values 22, 24 and 26 are obviously required for a correct decrypting of the multimedia data in a decryption device. This is why they have to be entered into the header 12 as will be explained later.

Fig. 2 shows a more detailed illustration of the encrypted multimedia data stream 10 consisting of the header 12 and

the payload data block 14. The header 12 is divided into several subblocks which will be explained especially referring to Fig. 3. It is pointed out that the number and the function of the subblocks can be extended at will.

5 Thus, in Fig. 2 some subblocks of the header 12 are illustrated in an only exemplary way. The header includes as it is shown in Fig. 2 a so-called crypt-block 29 comprising, in general terms, relevant information for encrypting the multimedia data. In addition the header 12
10 includes a so-called license block 30 comprising data referring to how a user can or is allowed to use the encrypted multimedia data stream. The header 12 further includes a payload data info block 32 which can include information concerning the payload data block 14 and as
15 well as general information about the header 12 itself. Furthermore the header 12 may comprise an old header block 34 enabling a so-called recursive header structure. This block makes it possible for the user who, apart from a decryption device is also in the possession of an
20 encryption device to reformat an encrypted multimedia data stream for other replay instruments in his possession without losing or modifying the original header information provided by the distributor. Depending on the application further subblocks, such as an IP information block (IP =
25 intellectual property) according to ISO/IEC 14496-1, MPEG-4, Systems, 1998, containing copyright information, can be added to the header 12.

As it is the standard in the art, an internal block
30 structure can be allocated to each block, this structure at first requesting a block identifier and including the length of the subblock and at last giving the block payload data itself. Thus, the encrypted multimedia data stream,

and in particular the header of the encrypted multimedia data stream, is given an increased flexibility in such a way that it can react to new requirements in such a way that additional subblocks may be added or existing subblocks may be omitted.

Fig. 3 gives an overview of the block payload data of the individual subblocks shown in Fig. 2.

At the beginning the crypt block 28 is explained. It contains an entry for a multimedia data encryption algorithm 40 identifying the symmetrical encryption algorithm used in the preferred embodiment, which has been used when encrypting the multimedia data. The entry 40 can be an index for a table in such a way that, after reading the entry 40, a decryption device is capable of selecting this encryption algorithm the encryption device has used from a plurality of encryption algorithms. The crypt block 28 further includes the entry first step 26, the entry step 24 and the entry amount 22, which has already been illustrated in connection with Fig. 1. These entries in the header enable a decryption device to subdivide an encrypted multimedia data stream accordingly to be able to carry out a correct decryption.

The crypt block 28 further contains an entry for the distributor or provider or supplier 42, the entry being a code for the distributor who has produced the encrypted multimedia data stream. An entry user 44 identifies the user who has obtained the encrypted multimedia data stream in some way from the distributor who is identified by the entry 42. It is a possible application of these identification codes to carry out the user identification

code in a device-specific way. The entry user would then contain the serial number of a PC, a laptop, a car hi-fi device, a home stereo system etc., allowing as replay on the specific instrument only. For a further increase of the flexibility and/or safety, a special identification code such as a logic linkage of the hard disk size and the processor number etc., in the example of a PC, could be employed instead of the serial number which looks different with every producer but may be identical accidentally.

The entry 46 contains an output value which will be discussed in detail later. This output value in general represents an encrypted version of the multimedia data key which, in connection with the multimedia data encryption algorithm identified by the entry 40, is required to decrypt the encrypted multimedia data (sections 16 in Fig. 1) present in the payload data block 14 correctly. In order to achieve a sufficient flexibility for future applications, the two entries output value length 48 and output value mask 50 are further provided. The entry output value length 48 illustrates the actual length of the output value 46. To achieve a flexible header format more bytes are however provided in the header format, for the output value than an output value actually comprises. The output value mask 50 thus illustrates how a shorter output value is distributed in a way on a longer output value place. If the output value length is for example half as big as the space available for the output value, the output value mask could be formed in such a way that the first half of the output value mask is set while the second half is masked. In this case the output value would simply be entered into the space provided for the header by the syntax and occupy

the first half while the other half would be ignored due to the output value mask 50.

Now the license block 30 of the header 12 will be explained. The license block includes an entry bit mask 52. This entry can comprise certain specific information for replaying or for the general way of using the encrypted multimedia data. With this entry a decryption device could especially be told whether the payload data can be replayed locally or not. In addition at this point it may be signalled whether the challenge response method has been used for the encryption, this method being described in the already mentioned German patent DE 196 25 635 C1 and enabling an efficient data base access.

An entry expiration date 54 indicates the point in time at which the permission to decrypt the encrypted multimedia data stream expires. A decryption device will in this case check the entry expiration date 54 and compare it to a build-in time measuring device in order not to carry out a decryption of the encrypted multimedia data stream if the expiration date has been exceeded. This makes it possible for the provider to make encrypted multimedia data available for a limited amount of time, which has the advantage of a much more flexible handling and price setting. This flexibility is further supported by an entry starting date 56 in which it is specified from which point on an encrypted multimedia file is allowed to be decrypted. An encryption device will compare the entry starting date with its built-in watch to only carry out a decryption of the encrypted multimedia data when the current point in time is later than the starting date 56.

The entry allowed replay number 58 indicates how often the encrypted multimedia data stream can be decrypted, that is replayed. This further increases the flexibility of the provider in such a way that it for example only allows a certain number of replays compared to a certain sum which is smaller than a sum which would arise for the unlimited usage of the encrypted multimedia data stream.

For verifying and supporting respectively the entry allowed replay number 58 the license block 30 further includes an entry actual replay number 60 which could be incremented by one for example after each decryption of the encrypted multimedia data stream. A decryption device will thus always check whether the entry actual replay number is smaller than the entry allowed replay number. If this is the case, a decryption of the multimedia data is carried out. If this is not the case, a decryption is no longer carried out.

Analog to the entries 58 and 60 entries allowed copy numbers 62 and actual copy number 64 are implemented. By means of the two entries 62 and 64 it is made sure that a user of the multimedia data only copies them as often as he or she is allowed to do so by the provider or as often as he or she has paid for when purchasing the multimedia data. By the entries 58 to 64 a more effective copyright protection is assured, a selection between private users and industrial users being attainable for example by setting the entries allowed replay number 58 and allowed copy numbers 62 to a smaller value.

The licensing could for example be designed in such a way that a certain number of copies (entry 62) of the original

are allowed while copies of a copy are not allowed. The header of a copy would then, unlike the header of the original, have zero as the entry allowed copy number in such a way that this copy can no longer be copied by a proper encryption/decryption device.

In the example for a multimedia data protection protocol (MMP) shown here the header 12 further contains a payload data information block 32 having in this case only two block payload data entries 66 and 68, the entry 66 containing a hash sum on the total header, while the entry 68 identifies the type of hash algorithm having been used for forming the hash sum on the total header.

In this context reference is made for example to "Applied Cryptography", Second Edition, John Wiley & Sons, Inc. by Bruce Schneider (ISBN 0 417-11709-9) including a detailed illustration of symmetrical encryption algorithms, asymmetrical encryption algorithms and hash algorithms.

The header 12 finally includes the old header block 34 which, along with the synchronizing information which is not shown in Fig. 3, comprises the entry old header 70. In the entry old header 70 the old header can be maintained by the provider if a user performs an encryption himself and thus produces a new header 12, in order not to lose essential information the provider has entered into the header. For this purpose author information (IP information block) could for example count prior user information and distributor information which enables tracing back of a multimedia file which for example has been decrypted and encrypted several times by different instruments to the original provider transparently, the author information

being maintained. It is thus possible to check at any point whether an encrypted multimedia file has been acquired legally or illegally.

- 5 After having explained the format of the encrypted multimedia data stream and various functionalities of encryption and decryption devices, the method according to the invention for encrypting multimedia data will now be explained referring to Fig. 4. In a preferred application
10 of the present invention the encryption method according to the invention is carried out at the distributor. The distributor preferably carries out a hybrid encryption method, that is a symmetrical encryption method for encrypting the multimedia data and an asymmetrical
15 encryption method for encrypting the multimedia data key.

A customer or user who wants to purchase multimedia data from a distributor at first contacts the distributor and, for example, tells him his credit card number to which the
20 distributor debits the payable amounts. Then the customer receives a table of the symmetrical encryption methods by the distributor. In addition the distributor and the customer exchange their respective public keys. If the user now orders a certain multimedia good from the distributor
25 the distributor performs a customer-selective encryption for this customer.

The detailed steps for producing the encrypted multimedia data stream could look the following way. The distributor
30 at first creates the header 12 for the multimedia file as far as it is possible until then (100). As can be seen from Fig. 3 the output value is not yet available at this point in time. For this reason the entry for the output value is

left empty in step 100 in which the header 12 is created as far as possible. All the other entries in the crypt block and all the other entries in the license block however do already exist. The hash sum or else the digital signature in the entry 66 on the total header however is not yet existent, which is why this entry is left empty. The entry old header 70 will very likely remain empty if the multimedia file is encrypted by the distributor for the first time. If, however, the distributor has acquired the encrypted multimedia file from another distributor, the entry 70 may already be filled. In a step 102 the distributor establishes a multimedia data key K which, together with the multimedia data encryption algorithm being identified by the entry 40 (Fig. 3), allows an encryption of the multimedia data, which is carried out in a step 104.

According to the present invention a hash sum on the header is formed, certain parts having a predefined value (step 106). The detailed illustration of the header in Fig. 3 at the right margin contains a column 107 which is to illustrate which parts or entries respectively in the header 12 receive a predefined value when forming a hash sum in step 106 (Fig. 4). The entry output value 64, the entry actual replay number 60, the entry actual copy number 64 and the entry hash sum on the header 66 and, under certain circumstances, the entry old header 70 especially receive a predefined value, as it is illustrated by the dotted cross for the entry 70. Certain parts of the header have to be given a pre-defined value when the hash sum is formed in step 106, since they are not yet fixed (output value 46) or are changed by a decryption device (entry 60 and 64). The entry 66, that is the hash sum on the header, is not yet

fixed either since the output value 46 is naturally also included in it.

5 The entries distributor 42, user 44 and the entries into the license block 30 are however included when forming the hash sum in step 106 (Fig. 4), whereby a personalization and protection respectively of the license block entries can be achieved since the hash sum obtained in step 106 is linked with the multimedia data key to obtain a basic value
10 (step 108).

Then the basic value obtained in step 108 is encrypted asymmetrically by means of the public key (0) of the customer (step 110). To render the encrypted multimedia
15 data stream to a transferable format, the header is finally completed (step 112) in such a way that the output value 46 is entered into the header already created in step 100.

Unlike the embodiment shown in Fig. 4, the order of the
20 steps can be exchanged. The entire encryption of the multimedia data key could for example be carried out first, the encryption of the multimedia data then being performed. In addition the hash sum on the header could be established before the multimedia data key is generated. Further
25 variations are possible. Step 108 can of course also be carried out after the hash sum has been established. Furthermore step 110 may only be carried out after a basic value has been established.

30 A symmetrical encryption method is preferable used for encrypting the multimedia data with the multimedia data key in step 104 since, in this case, relatively large amounts of data have to be encrypted and decrypted. Symmetrical

encryption methods, as is well known, are faster than asymmetrical encryption methods as they are employed in step 110 for encrypting the multimedia data key.

5 It is also preferred that the multimedia data key K is generated by means of a random number generator in such a way that the basic value generated in step 108 always takes a different form for one and the same customer to make an attack on the cryptographic system as difficult as possible.
10

The linkage operation to link the hash sum and the multimedia data key K should, as will be explained referring to Fig. 5, be a self-inverse linkage. Such a self-inverse linkage would be the XOR-linkage. Self-inverse means that applying this linkage two times yields a result equal to the output value. It is also possible that the linkage function of Fig. 5 is the inverse function of that of Fig. 4. The linkage function thus only has to be reversible, that is there must be a reverse function of it.
15
20

In step 110 an asymmetrical encryption method is carried out according to the invention. As it is known, there are two keys in an asymmetrical encryption method, with the help of which an encryption and decryption respectively are possible, the keys being different from each other. One key is called private key P while the other key is called public key O. Asymmetrical encryption methods in general have the property that data to be encrypted having been encrypted by means of the private key can be decrypted again by the public key. In an analog way data to be encrypted having been encrypted by means of the public key are decrypted again by means of the private key. Thus it
25
30

can be deduced that the private and public keys are in general exchangeable.

5 An aspect of the present invention is that the header on the steps 106 and 108 is included in the encryption of the multimedia data key. Alternatively parts of the payload data block may also be included, whereby the entire multimedia data stream would become useless due to a disallowed manipulation of the payload data since it will
10 no longer be possible in this case to calculate the multimedia data key in the decryption device.

Although it has been mentioned in step 106 that a hash sum on the header is formed, it is also pointed out that each
15 processing of a part of the multimedia data stream to derive information marking the part of the multimedia data stream can be employed. The more complicated the hash algorithm used herein is, the safer the encrypted multimedia data stream will be from attackers who want to
20 crack it to modify the license information and the distributor or user information respectively for example for their (illegal) purposes.

Now reference is made to Fig. 5 which shows a flow chart of
25 the decryption method which is possibly performed by a customer. In a step 120 the customer at first reads the output value from the header of the encrypted multimedia data stream. Then he performs a decryption of this output value by means of the respective asymmetrical decryption
30 (step 122). Then the decryption device at the customer forms a hash sum on the header, certain parts which had predefined values when encrypted also receiving the same predefined value in a step 124. Then the hash sum with the

decrypted output value (step 122) is linked, whereby the multimedia data key is formed (step 126). In a step 128 the encrypted multimedia data is finally decrypted by means of the multimedia data key obtained in step 126.

5

It is evident that the decryption method is basically the reversal of the encryption method having been described referring to the flow chart of Fig. 4. In the decryption method shown in Fig. 5 several steps may also be exchanged.

10 Thus, the hash sum on the header could for example be formed (124), after which the output value is decrypted by means of the public key (step 122). Reading the output value from the header (step 120) could for example be performed after step 124 but in any case in front of step
15 126. Step 128 will only be possible after step 126 has been performed since it yields the multimedia data key.

The decryption method shown in Fig. 5 expresses by means of step 124, what will happen if a customer modifies the
20 header 12 which is usually unencrypted and very easily susceptible for attackers. A change of the license information of the beginning and the end dates for example would however inevitably result in the hash sum on the header, formed in step 124, having a different value than
25 the hash sum formed in step 106 (Fig. 4) during the encryption. The repeated linkage of the hash sum in step 126 (Fig. 5) will thus no longer result in the correct multimedia data key since the two hash sums, that is the hash sum during the encryption and the hash sum during the
30 decryption, are different from each other. Thus the entire multimedia data is useless since it can no longer be decrypted correctly since it is no longer possible, due to the manipulation of the header, to calculate the multimedia

data key the encryption device has employed. Any change of the header thus automatically leads to the destruction of the multimedia data itself.

SECRET

Claims

1. Method for producing a payload data stream (10) comprising a header (12) and a payload data block (14) containing encrypted payload data, comprising the following steps:

generating (102) a payload data key for a payload data encryption algorithm for encrypting payload data;

encrypting (104) payload data using said payload data key and said payload data encryption algorithm to obtain an encrypted section (16) of said payload data block (14) of said payload data stream (10);

processing (106) a part of said payload data stream (10) to deduce information marking said part of said payload data stream;

linking (108) said information containing said payload data key by means of an invertible logic linkage to obtain a basic value;

encrypting (110) said basic value using a key of two keys (P, O) being different from each other by an asymmetrical encryption method, said two different keys being the public (O) and the private (P) keys respectively for said asymmetrical encryption method, to obtain an output value (46) being an encrypted version of said payload data key; and

entering (112) said output value (46) into said header (12) of said payload data stream (10).

5 2. Method according to claim 1, in which said payload data encryption algorithm is a symmetrical encryption algorithm.

10 3. Method according to claim 1 or 2, in which said invertible logic linkage is self-inverting and includes an XOR-linkage.

15 4. Method according to one of the preceding claims, in which one key of said two keys (P, O) being different from each other is the private key (P) of a producer of said payload data stream or the public key (O) of a consumer of said payload data stream.

20 5. Method according to one of the preceding claims, in which said part of said payload data stream being processed (106) to deduce said information includes at least a part of said header (12).

25 6. Method according to one of the preceding claims, in which said step of processing (106) comprises forming a hash sum.

30 7. Method according to one of the preceding claims, further comprising the following step:
identifying said algorithm being used in said step of processing (106) by an entry (68) into said header.

8. Method according to one of the preceding claims, further comprising the following step:

entering license data (30) into said header (12), said data referring to in which way said payload data stream (10) is allowed to be employed.

9. Method according to claim 8, in which said license data (30) indicates how often said payload data stream is allowed to be replayed (58) and how often it has already been replayed (60).

10. Method according to claim 8 or 9, in which said license data (30) indicates how often the contents of said payload data stream is allowed to be copied (62) and how often it has already been copied (64).

11. Method according to one of claims 8 to 10, in which said license data (30) indicates from when on said payload data stream is no longer allowed to be employed (54).

12. Method according to one of claims 8 to 11, in which said license data (30) indicates from when on said payload data stream is allowed to be decrypted (56).

13. Method according to one of claims 8 to 12, in which said part of said payload data stream being processed to deduce said information (106) includes said license data (30).

14. Method according to one of the preceding claims, in which said step of processing further comprises the following substep:

5 setting said entry (46) for said output value in said header (12) to a defined value and processing (106) said entire header, including said entry (46) set to a defined value.

- 10 15. Method according to one of the preceding claims, further comprising the following steps:

 identifying the supplier (42) of said payload data stream by a supplier entry (42) into said header (12);

15 identifying the user (44) of said payload data stream by a user entry (44) into said header (12) of said payload data stream,

20 said supplier entry (42) and said user entry (44) belonging to said part of said payload data stream (10) being processed (106) to deduce said information.

- 25 16. Method according to one of the preceding claims, further comprising the following step:

 identifying said payload data encryption algorithm by an entry (40) into said header (12) of said payload data stream (10).

30

17. Method for decrypting an encrypted payload data stream (10) comprising a header (12) and a payload data block (14) containing encrypted payload data, said header

(12) comprising an output value (46) having been generated by an encryption of a basic value by an asymmetrical encryption method using a key of two different keys (P, O) including a private (P) and a public (O) key, said basic value representing a linkage of a payload data key, with which said encrypted payload data is encrypted using a payload data encryption algorithm, and information deduced by a certain processing, said information marking a certain part of said payload data stream (10) unambiguously, said method comprising the following steps:

obtaining (120) said output value (46) from said header (12);

decrypting (122) said output value (46) using the other key of said asymmetrical encryption method to obtain said basic value;

processing (124) a part of said payload data stream (10) using the processing method used for encrypting to deduce information marking said part, said part corresponding to said certain part when encrypting;

linking (126) said information and said basic value using the corresponding linkage as it has been used when encrypting to obtain said payload data key; and

decrypting (128) said block (14) containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting.

18. Method according to claim 17, in which said header (12) comprises license information (30) referring to in what way said payload data stream (10) can be employed.

19. Method according to claim 17 or 18, in which said part being processed to deduce said information is said header (12).

20. Method according to claim 18 or 19, further comprising the following steps:

checking whether said license information (30) allows a decryption; and

if a decryption is not allowed, cancelling said decryption method.

21. Method according to one of claims 17 to 20, in which said header (12) comprises a user entry (44), said method further comprising the following steps:

checking by means of said user entry (44) whether a current user is authorized; and

if the user is not authorized, cancelling said decryption method.

22. Method according to one of claims 17 to 21, in which one key having been used when encrypting is the private key (P) of said asymmetrical encryption method, while the other key having been used when

decrypting is the public key (O) of said asymmetrical encryption method.

23. Method according to one of claims 17 to 21, in which
5 one key having been used when encrypting is the public key (O) of said asymmetrical encryption method, while the other key having been used when decrypting is the private key (P) of said asymmetrical encryption method.
24. Method according to one of claims 17 to 23, in which
10 said step of processing (124) includes forming a hash sum.
25. Method according to one of claims 17 to 24, in which a
15 part of said header (12) having been set to a defined value for said step of processing when encrypting is set to the same defined value for said step of processing (124) when decrypting.
26. Method according to claim 25, in which said part of
20 said header (12) being set to a defined value includes said entry for said output value (46) of said header (12).
27. Method according to one of claims 17 to 26, in which
25 said step of linking (126) comprises using an XOR-linkage.
28. Device for producing an encrypted payload data stream
30 comprising a header (12) and a payload data block (14) containing encrypted payload data, comprising:

means for generating (102) a payload data key for a payload data encryption algorithm for encrypting said payload data;

5 means for encrypting (104) payload data using said payload data key and said payload data encryption algorithm to obtain an encrypted section (16) of said payload data block (14) of said payload data stream (10);

10 means for processing (106) a part of said payload data stream (10) to deduce information marking said part of said payload data stream;

15 means for linking (108) said information and said payload data key by means of an invertible logic linkage to obtain a basic value;

20 means for encrypting (110) said basic value using a key of two keys (P, O) being different from each other by an asymmetrical encryption method, said two different keys being the public (O) and the private (P) keys respectively for said asymmetrical encryption method to obtain an output value (46) being an
25 encrypted version of said payload data key; and

means for entering (112) said output value (46) into said header (129 of said payload data stream (10)).

30 29. Device for decrypting an encrypted payload data stream (10) comprising a header (12) and a block (14) containing encrypted payload data, said header (12) comprising an output value (46) having been generated

by an encryption of a basic value by an asymmetrical encryption method using a key of two different keys (P, O) including a private (P) and a public (O) key, said basic value representing a linkage of a payload data key, with which said encrypted payload data is encrypted using a payload data encryption algorithm, and information deduced by a certain processing, said information marking a certain part of said payload data stream (10) unambiguously, said device further comprising:

means for obtaining (120) said output value (46) from said header (12);

means for decrypting (122) said output value (46) using said other key (O) and said asymmetrical encryption method to obtain said basic value;

means for processing (124) a part of said payload data stream (10) using the processing method used when encrypting to deduce information marking said part, said part corresponding to said certain part when encrypting;

means for linking (126) said information and said basic value using the corresponding linkage as it has been used when encrypting to obtain said payload data key; and

means for decrypting (128) said block (14) containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting.

30. Device according to claim 28 or 29, which is implemented as a personal computer, a stereo system, a car hi-fi instrument, a solid state player or a replay instrument containing a hard disk or a CD-ROM.

Method and device for producing an encrypted payload data stream and method and device for decrypting an encrypted payload data stream

5

Abstract

In a method for producing an encrypted method payload data stream comprising a header and a block containing encrypted payload data, a payload data key for a payload data encryption algorithm for encrypting payload data (102) is generated. The payload data is encrypted using the generated payload data key and the payload data encryption algorithm (104) to obtain the block containing the encrypted payload data of the payload stream. A part of the payload data stream is processed (106) to deduce information marking the part of the payload data stream. The information is linked (108) with the payload data by means of an invertible logic linkage to obtain a basic value. This basic value is finally encrypted (110) using a key of two keys being different from each other by an asymmetrical encryption method, the two different keys being the public and the private keys respectively for the asymmetrical encryption method to obtain an output value being an encrypted version of the payload data key. The output value is finally entered into the header to complete (112) the payload stream. Changes of the header and of the payload data itself, which are not authorized, lead to an automatic destruction of the payload data.

30



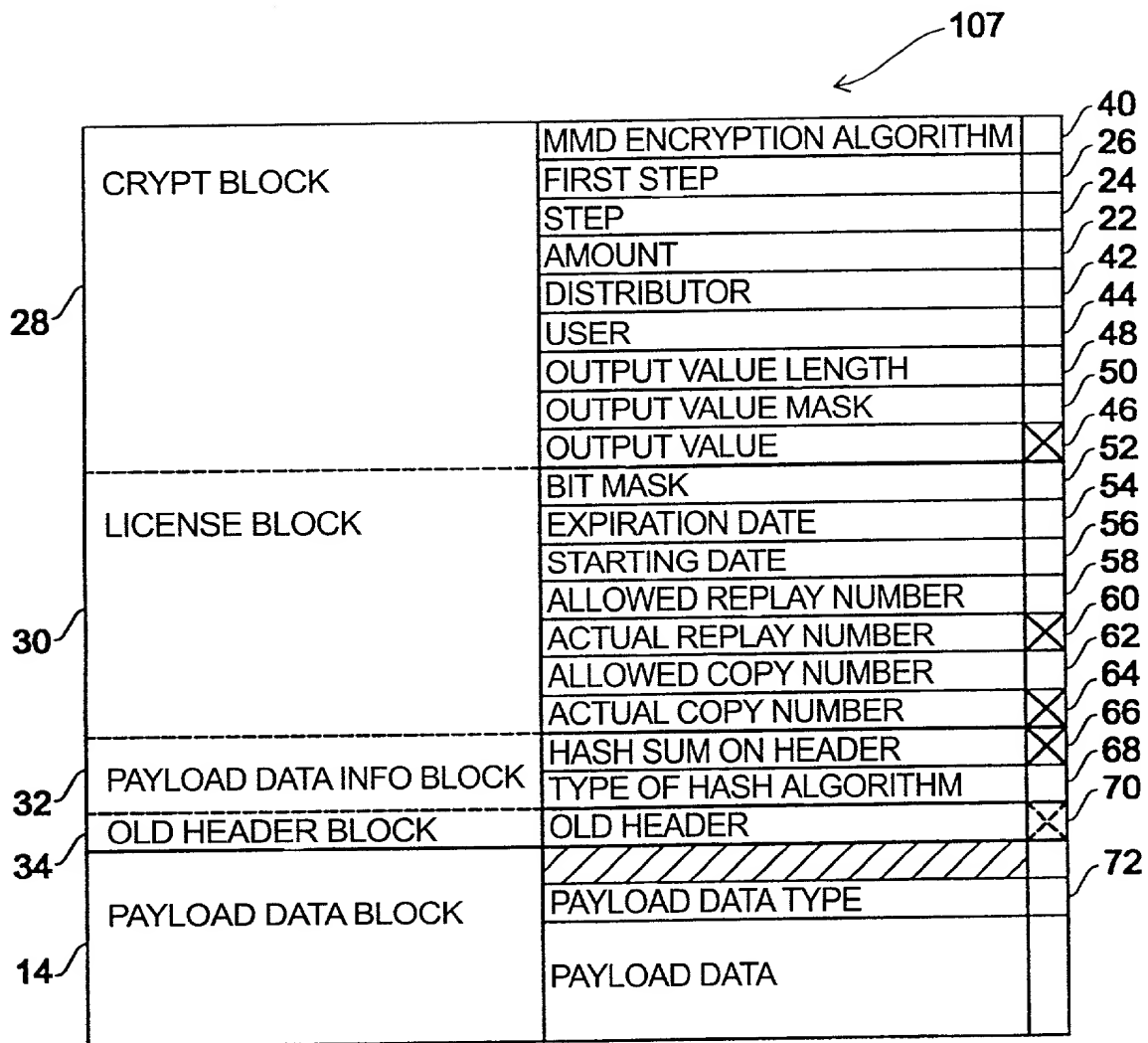


Fig. 3

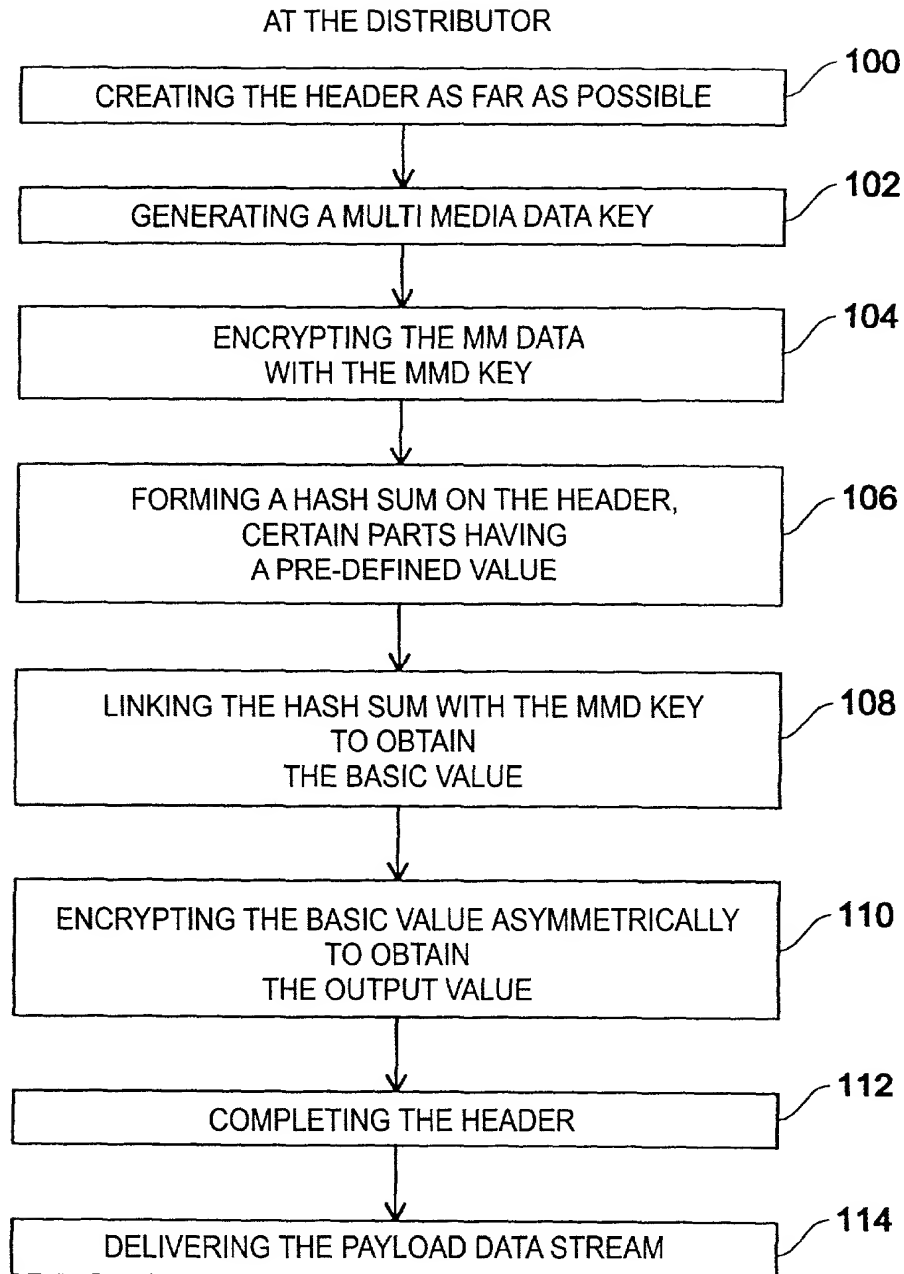


Fig. 4

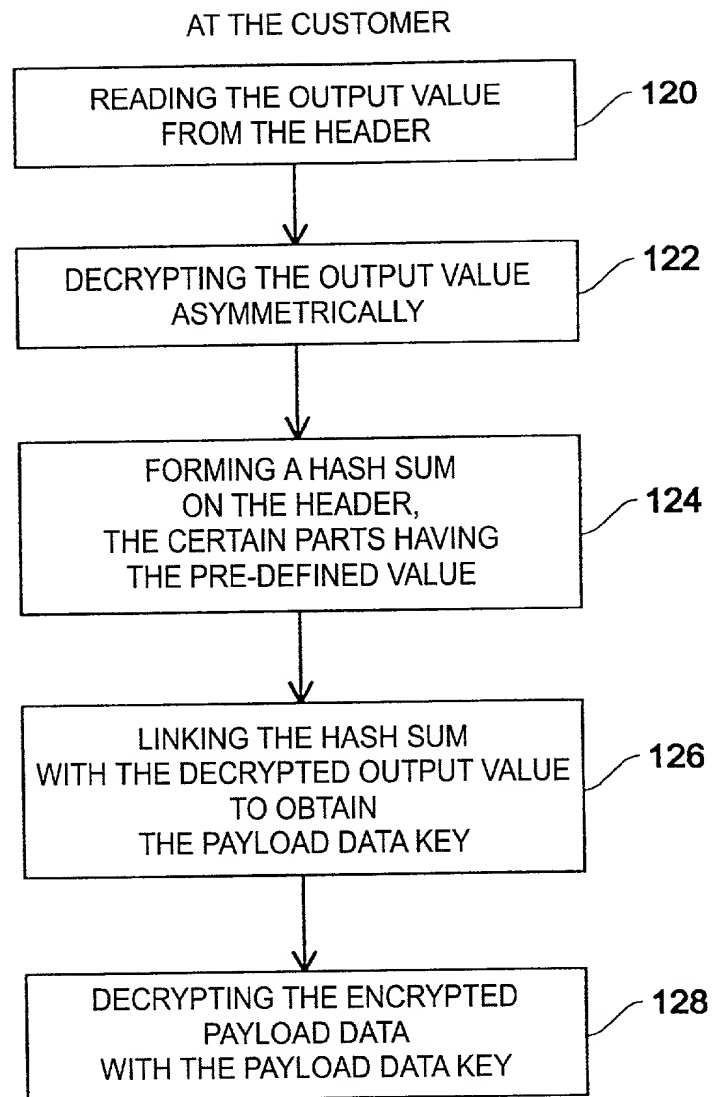


Fig. 5

COMBINED DECLARATION AND POWER OF ATTORNEY

**(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL,
CONTINUATION, OR C-I-P)**

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for a national stage of PCT application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

METHOD AND DEVICE FOR PRODUCING AN ENCRYPTED PAYLOAD DATA STREAM AND
METHOD AND DEVICE FOR DECRYPTING AN ENCRYPTED PAYLOAD DATA STREAM

SPECIFICATION IDENTIFICATION

The specification was filed on August 16, 2001, as Serial No. 09/913,686

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

PRIORITY CLAIM (35 U.S.C. Section 119(a)-(d))

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

Such applications have been filed as follows.

**PRIOR PCT APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

INDICATE IF PCT	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
PCT	PCT/EP99/09981	15 December 1999	yes

**PRIOR FOREIGN APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
Germany	19906450.4	16 February 1999	yes

POWER OF ATTORNEY

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer No. 24283

SEND CORRESPONDENCE TO:

Customer No. 24283

DIRECT TELEPHONE CALLS TO:

Carl A. Forest
303-379-1114

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Niels Rump

Inventor's signature _____

Date _____

Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address Brueckenstrasse 13, Erlangen D-91056 Germany

200

Juergen Koller

Inventor's signature _____

Date September 24, 2001

Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address St. Johann 6/113, Erlangen D-91054 Germany

300

Karlheinz Brandenburg

Inventor's signature _____

Date September 24, 2001

Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address Haagstrasse 32, Erlangen D-91054 Germany

204210-93361550

**SIGNATURE BY JOINT INVENTOR(S) ON BEHALF OF NONSIGNING
INVENTOR(S) WHO CANNOT BE REACHED
(37 C.F.R. section 1.47(a))**

- I.** I am an above named joint inventor and have signed this declaration on my own behalf and also sign this declaration under 37 C.F.R. section 1.47(a) on behalf of the nonsigning joint inventor, particulars for whom are:

Niels Rump, nonsigning inventor who cannot be found or reached.

Country of Citizenship of nonsigning inventor:

Germany

Last known address of nonsigning inventor:

Brueckenstrasse 13

Erlagen, D-91056 Germany

- II.** Accompanying this declaration is:

- (1) A STATEMENT OF FACTS IN SUPPORT OF FILING ON BEHALF OF NONSIGNING INVENTOR.
- (2) THE PETITION FEE OF \$130.00 (37 C.F.R. Section 1.17(i)).

Date: September 24, 2001


Signature Juergen Koller

Date: September 24, 2001


Signature Karlheinz Brandenburg

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Niels Rump, Juergen Koller, Karlheinz Brandenburg

For: METHOD AND DEVICE FOR PRODUCING AN ENCRYPTED PAYLOAD DATA STREAM
AND METHOD AND DEVICE FOR DECRYPTING AN ENCRYPTED PAYLOAD DATA
STREAM

The specification of which was filed on August 16, 2001, as Application No. 09/913,686.

**STATEMENT OF FACTS IN SUPPORT OF FILING
ON BEHALF OF NONSIGNING INVENTOR (37 C.F.R. SECTION 1.47)**

This statement is made as to the exact facts that are relied upon to establish the diligent effort made to secure the execution of the declaration by the nonsigning inventor for the above identified patent application before deposit thereof in the Patent and Trademark Office.

Because signing on behalf of the nonsigning inventor is by a person or entity showing a sufficient proprietary interest, this statement also recites facts as to why this action was necessary to preserve the rights of the parties or to prevent irreparable damage.

This statement is being made by the available person having first-hand knowledge of the facts recited therein.

IDENTIFICATION OF PERSON MAKING THIS STATEMENT OF FACTS

Fritz Schoppe
Schoppe, Zimmermann, Stöckeler & Zinkler
Patentanwälte
Irmgardstrasse 22
München D-81479
Germany

**EFFORTS DURING CONVENTION YEAR TO PREPARE APPLICATION AND
OBTAIN INVENTOR'S SIGNATURE**

See attached sheet

LAST KNOWN ADDRESS OF THE NONSIGNING INVENTOR

Niels Rump
Brueckenstrasse 13
Erlagen D-91056
Germany

DETAILS OF EFFORTS TO REACH NONSIGNING INVENTOR

See attached sheet

**DETAILS OF REFUSAL OF NONSIGNING INVENTOR
TO SIGN APPLICATION PAPERS**

N/A

**PROOF OF NEED TO PREVENT IRREPARABLE DAMAGE
OR PRESERVE THE RIGHTS OF THE PARTIES**

The National Phase filing date in the United States Patent Office of PCT Application PCT/EP99/09981 expired August 16, 2001. The application was filed with no signatures. The nonsigning inventor still cannot be found.

Date: September 24, 2001



Signature of person making statement

IN THE UNITED STATES ELECTED OFFICE (EO/US)

PCT/EP99/09981	15 December 1999 (15.12.99)	16 February 1999 (16.02.99)
International Application Number	International Filing Date	International Earliest Priority Date

U.S. Application Serial No.: 09/913,686

Filing Date: 16 Aug 2001

TITLE OF INVENTION: METHOD AND DEVICE FOR PRODUCING AN ENCRYPTED
PAYLOAD DATA STREAM AND METHOD AND DEVICE FOR
DECRYPTING AN ENCRYPTED PAYLOAD DATA STREAM

APPLICANT(S): Rump, Niels; Koller, Juergen and Brandenburg, Karlheinz

ATTACHMENT TO STATEMENT OF FACTS

Following are the details of the efforts to reach inventor Niels Rump:

1. A letter was mailed to Niels Rump at his last known address of Brückenstrasse 13, D-91056 Erlangen on June 27, 2001, which included a Combined Declaration And Power Of Attorney and Assignment Of Invention. A copy of the letter is attached. The package was returned by mail stating "Address Unknown". A copy the labeled envelope is also attached.
2. On July 2, 2001, a letter was mailed addressed to the family of Mr. Rump at the same address. This letter was returned by mail also stating "Address Unknown". Copies of the letter and the labeled envelope are attached.
3. A request has been submitted with the residence registration office in Erlangen in an attempt to locate Mr. Niels Rump. The request revealed nothing else as the last known address in Erlangen cited above.
4. Finally, a request was submitted with the telephone inquiry office which revealed that Mr. Niels Rump was not registered in Erlangen.